

TIPS TO AVOID INTERNET BANKING FRAUDS

Last week, Mr. Kumar from Delhi checked his bank account and he was in for a shock. A whopping sum of INR 1.66 Crores was missing. The transactions of this big amount had taken place over a period of over 5 transaction days.

But he is not the only victim of Net banking fraud. According to Delhi Police every year, around 200 complaints are received and the figure is rising though only few cases are actually registered. This goes on to show that the Net banking convenience has its set of risks too. The stepping of financial institutions into the virtual realm has lead to a new breed of financial criminals. Criminals largely thrive on the lack of knowledge of net users and technology loopholes.

So, here's how cyber thieves hijack your money and how you can guard against Net banking frauds.

Some cases & manners of Crime

Phishing

A person's personal details are obtained by fraudsters posing as bankers, who float a site similar to that of the person's bank. They are asked to provide all personal information about themselves and their account to the bank on the pretext of database upgradation. The number and password are then used to carry out transactions on their behalf without their knowledge.

One of the prominent cases of phishing involved six bank accounts from where money was withdrawn by two persons, including a Nigerian national, in August this year. The two were later arrested by the Delhi Police. The phishing site of the 'A Bank' was created somewhere in Nigeria in collusion with another Nigerian identified as Kenneth (name changed) in India. Kenneth roped in Arun Kumar (name changed) who had an account at the 'A bank'. The Nigerian used to buy grocery from Kumar's shop and told him that if Kumar provided him with his bank account number, he would immediately pay off his pending grocery bills and give some extra money as well.

As soon as Kumar parted with his details, someone in Nigeria floated a fake website of 'A Bank'. He then sent emails to six people at different places in India, asking about their account details on the pretext of data upgradation. Once the details came in, the person in Nigeria transferred money into Kumar's account from the other six accounts through Net banking. Next morning, Kumar went to the branch at Khan Market to withdraw the money but the bank official grew suspicious and detained him.

Hacking

Here, personal data is stolen through hacking. The fraudster needs to be an adept cyber criminal who can steal information stored or transacted in any computer. Sometimes, a spyware is installed in computer to gain access to all files.

A senior police official explaining the modus operandi of hackers said, "A hacker is much more than an average thief. He gets into the system with the help of a spyware and steals information. The hacker is always on the lookout for unsecured systems and files. The spyware usually comes in the form of a virus. This spy transports all files pertaining to bank accounts to the hacker. Therefore, it is advisable not to store much information about your accounts on your computer or email which is unsecured."

Public PC's

Also, using Net banking services at cyber cafes leaves one vulnerable to data thieves. Another modus operandi adopted by cheats these days is stealing data from public computers or shared PCs. The fraud here takes advantage of unsecured cyber cafes. A police officer says, "Sometimes, the cafe owners are hand-in-glove with the thugs."

Some simple tips to prevent you from falling into the trap of cyber criminals.

A simple ignorance or oversight can make a huge dent in your hard-earned savings, so be cautious.

- ❏ Avoid online banking on unsecured wifi systems and operate only from PCs at home.
- ❏ Never reveal password to anyone. Do not even write it on a piece of paper or diary. Just memorize it.
- ❏ Change your online banking password at regular intervals.
- ❏ Also, avoid easy-to-guess passwords, like first names, birthdays, kid's or spouse's name and telephone numbers. Try to have an alpha-numeric password, one that combines alphabets and numbers.
- ❏ If you have several bank accounts, never use the same online banking password for all.
- ❏ Never select the option on browser that stores or retains user name and password, As it can easily be cracked by cyber criminals.
- ❏ Also, never paste your password, always type it in. This little amount of 'finger exercise' will go a long way in safety.
- ❏ Never reply to queries from bank online about account or personal details. The personal information should not be kept in a public computer or in emails.
- ❏ Always check the URL of your bank's web site. Fraudsters can lure you to enter your user ID and password at a fake website that resembles your bank. If you see anything other than the bank's genuine URL, it has to be fake.
- ❏ Never enter your user ID or password or such sensitive information without ascertaining that you are on the right website.
- ❏ Always type the Web address of your bank into the browser address space. Never click on the link in the email.
- ❏ Most banks have a 'last logged in' panel on their websites. If your bank has it, check the panel whenever you log in. If you notice irregularities (like you are logging in after two days, but the panel says you logged in that morning!), report the matter immediately to your bank and change your password right-away.

- ❏ Always log out when you exit the online banking portal. Close the browser to ensure that your secure session is terminated. Never exit simply by closing the browser.
- ❏ Regularly check for security updates for your computer operating system. Most security updates are aimed at reducing risks to your computer, these may be data-related or otherwise. Make sure that your operating system and browser have the latest security patches installed. And, always install these only from trusted websites.
- ❏ Install a personal firewall to prevent hackers from gaining unauthorized access to your computer, especially if you connect to the Internet through a cable or a DSL modem.
- ❏ Don't leave the PC unattended after keying in information while transacting on the website. Avoid accessing your bank online at cyber cafes or on a share or public computer.
- ❏ Also, avoid locations that offer online connections through wireless networks (Wi-Fi), where privacy and security are minimal.

What the Banks say?

- ❏ Banks say that appropriate up-gradations are carried out from time to time by their IT departments for risk mitigation.
- ❏ They issue instructions to the customers to manage their accounts through virtual keyboards by way of which the characters typed by them are not identified by hackers.
- ❏ SMS alerts are also an important tool since any transaction carried out on account is reported to the account holder through an SMS.